

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY**

THE HOMESOURCE, CORP. Plaintiff, vs. RETAILER WEB SERVICES, LLC and JOHN DOES 1-3, Defendants.	Case No. 1:18-cv-11970
---	------------------------

FIRST AMENDED COMPLAINT

1. Plaintiff The HomeSource, Corp. (“HomeSource”) hereby amends its Complaint as of right pursuant to Federal Rule of Civil Procedure 15(a)(1)(B) to assert additional claims against defendant John Does 1-3. HomeSource does not yet know the identity of John Does 1-3 (or whether they share the same identity), but will seek this information through discovery.

2. HomeSource filed its initial complaint against defendant Retailer Web Services, LLC (“RWS”) for false advertising, defamation, tortious interference with commercial relationships, and unfair competition. Both HomeSource and RWS provide competitive technology services, including but not limited to operating websites for the same types of retail store customers.

3. In late 2017, HomeSource launched a product that directly competes with RWS’s product and began to quickly acquire RWS customers. On July 16, 2018, for example, HomeSource moved approximately 200 customers from RWS’s platform to HomeSource’s platform.

4. The same day, RWS began a smear campaign designed to unfairly disparage HomeSource and deceive its customers. RWS published false and misleading statements about

HomeSource in newsletters distributed via email over the next few days to HomeSource's customers and potential customers. RWS further contacted HomeSource's customers and potential customers by telephone regarding the same issues.

5. On or about July 19, 2018, RWS misrepresented security vulnerabilities of HomeSource's data and intellectual property to third parties. RWS emailed HomeSource notice of a "security hole" in HomeSource's software at 11:59 p.m., and then uploaded a video at 1:33 a.m. just hours later advertising the "security hole" to the public.

6. On July 20, 2018, RWS sent out the newsletter attached as Exhibit A to the parties' customers and potential customers. This lawsuit followed on July 23.

7. Beginning on or about August 9, 2018, John Doe 1 (hereinafter referred to as "Cyber-Attack Doe"), engaged in a series of denial of service ("DoS") and/or distributed denial of service ("DDoS") attacks on HomeSource's customers' websites, in an apparent effort to slow down, interrupt, and/or crash those websites.

8. HomeSource was able to successfully block these attacks within a few days.

9. Immediately thereafter (after the close of business on August 13), John Doe 2 (hereinafter referred to as "Hacking Doe") attempted to "hack" into HomeSource's platform, or to gain unauthorized access to HomeSource's customer data. On August 13, 2018, at 9:02 pm, RWS's CEO, Jim Kane, sent HomeSource an email notifying HomeSource of the hacking attempt, stating:

"We have observed that the following websites...which we believe to be operated by HomeSource, appear to have been compromised by a third party (see attached screen shots). We wanted to let you know as a professional courtesy in case any customer information has been compromised."

10. Hacking Doe's attack occurred the night before HomeSource had a meeting to show a new potential customer (and current large customer of RWS) its platform.

11. The only HomeSource customers targeted by Hacking Doe appear to be HomeSource customers that are former RWS customers. HomeSource possesses evidence that Hacking Doe was working from a specific, non-public list of former RWS customers.

12. To complete the attack, Hacking Doe manually entered information that was only available to RWS and HomeSource. Specifically, Hacking Doe entered in the website addresses and IP addresses of customers that had switched from RWS to HomeSource, even where that information was not publicly available.

13. On or about August 18, 2018, HomeSource was notified that John Doe 3 (hereinafter "Fake-Customer Doe") was sending emails to HomeSource's customers complaining about HomeSource's website functionality. A copy of one such email (from misc@aol.com) is attached hereto as Exhibit B.

14. Following the receipt of the email attached hereto as Exhibit B, HomeSource investigated the Internet activity of Fake-Customer Doe and uncovered evidence that Fake-Customer Doe's claims in Exhibit B are false. HomeSource also uncovered that Fake-Customer Doe went to great lengths to hide its digital fingerprints – something a normal consumer would ordinarily not do or know how to do.

15. On or about August 27, 2018, Cyber-Attack Doe launched another set of DoS and/or DDoS attacks through the use of bots, using a different method.

16. HomeSource also shut down these attacks, using a different method.

17. In doing so, and as set forth more fully below, HomeSource observed an exponentially disproportionate amount of website traffic coming from Scottsdale, Arizona. This

traffic originated from the location set forth in Exhibit C, which appears to be within a mile of RWS's office.

18. HomeSource brings this first amended complaint against Cyber-Attack Doe and Hacking Doe for tortious interference with commercial relationships and violations of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030. HomeSource asserts an additional claim for tortious interference with commercial relationships against Fake-Customer Doe.

19. As a result of RWS's and John Doe 1-3's unlawful actions, HomeSource has lost customers and its reputation has been unfairly damaged in an amount to be determined at trial.

PARTIES

20. Plaintiff HomeSource is a New Jersey corporation with its principal place of business at 420 Ganttown Road, Sewell, NJ 08080.

21. Defendant RWS is an Arizona limited liability company with a principal place of business at 15615 N. 71ST Street, Suite 205, Scottsdale, AZ 85254.

22. Defendant RWS's statutory registered agent is: Kingsley Law Firm PLC, 14362 N. Frank Lloyd Wright BLVD, #1000, Scottsdale, AZ 85260.

23. At this time, HomeSource does not know the identity of the defendant Does. When that information is known, HomeSource will amend its pleading to identify that person/entity and any other person/entity associated with that person.

24. HomeSource attempted to "trace" the location of the defendant Does without the benefit of any discovery by analyzing the volume and origin of all web traffic since RWS sent the newsletter and emails in mid July 2018.

25. HomeSource uncovered over 114,000 requests to access/search their customers' websites from Arizona, and approximately 38,000 requests within a mile of RWS's main office.

26. On average, many of HomeSource's customers' websites see 150-300 users per day.

27. HomeSource does not have any information yet confirming the location of Hacking Doe or Fake-Customer Doe.

JURISDICTION AND VENUE

28. This Court has federal question jurisdiction over HomeSource's federal claims pursuant to 28 U.S.C. §§ 1331, 1338(a).

29. This court has personal jurisdiction over defendant RWS because RWS is engaged in the systematic and continuous conduct of business in the State of New Jersey. RWS's conduct in connection with the State of New Jersey required it reasonably to anticipate that it would be subject to the jurisdiction of the courts in the State of New Jersey.

30. Upon information and belief, this court has personal jurisdiction over defendant Does because Does expressly aimed tortious conduct at HomeSource, a New Jersey corporation, via the internet such that defendant Does could reasonably anticipate being haled into district court in New Jersey due to their tortious conduct.

31. Venue in the District of New Jersey is proper under 28 U.S.C. § 1391.

FACTUAL BACKGROUND

A. HomeSource and RWS

32. HomeSource provides software and data solutions for retailers and manufacturers.

33. HomeSource's proprietary software aggregates large amounts of data – including item numbers, product specs, training videos, and more – into one single, usable platform, which allows retailers and manufacturers to streamline various processes such as printing customized quotes, providing accurate shipping times, and real-time updating of sizes, colors, and options so dealers always have current and accurate information at their fingertips.

34. Upon information and belief, RWS offers a competitive tool called “RetailDeck/WebFronts.”

35. Recently, GridIron Capital (“GridIron”), and its subsidiary Nationwide Marketing Group (“Nationwide”), considered investing in HomeSource, and all three parties entered into a non-disclosure agreement (“NDA”).

36. Through the due diligence process, GridIron and Nationwide acquired a great deal of sensitive, proprietary information about HomeSource, its software, financial reports, and legal history.

37. GridIron and Nationwide ended up not investing in HomeSource, but they did invest in RWS, according to a press release from February 24, 2018.

38. Recently, several companies, including Appliance Dealers Cooperative (“ADC”) and its members, have switched from using RWS’s “RetailDeck/WebFronts” platform to using HomeSource’s platform.

B. RWS’s False and Misleading Advertising and Tortious Interference

39. On or about July 20, 2018, RWS’s CEO Jim Kane and COO Jennie Gilbert emailed a newsletter to HomeSource’s customers and potential customers which contained materially false and misleading statements about HomeSource. *See* July 20th Newsletter, attached as Exhibit A.

40. Under the heading, “Has HomeSource ever done anything like this before?”, RWS stated, “The White family, owners of HomeSource and similar other businesses, appear to have a history of their business relationships ending in lawsuits against them. They were found guilty of making **negligent misrepresentations about the capabilities of their software in a federal lawsuit** (Civil Action NO. 3:12-CV-0090).”

41. The text “Civil Action NO. 3:12-CV-0090” contains a hyperlink to Judge Graham Mullen’s Order (“Graham Order”) on a motion for attorney’s fees in the case of *Furniture Distributors, Inc. v. Software Support-PMW, Inc.* (“Furniture Lawsuit”).

42. HomeSource was not a party in the Furniture Lawsuit and was not found “guilty” of making negligent misrepresentations about the capability of their software.

43. No member of the White family was a party in the Furniture Lawsuit, and no member of the White family was found “guilty” of making negligent misrepresentations about the capability of their software.

44. RWS further misrepresented: “The judge later deemed the counter-claims they alleged along the way ‘totally meritless’ and ordered them to pay Furniture Distributors, Inc. fifty thousand dollars to reimburse attorney fees in addition to the four hundred fifty thousand dollars already awarded them at trial.”

45. RWS’s use of “they” implies that HomeSource and the White family filed these counterclaims, but once again, they were not parties to the lawsuit, and it was actually Software Support-PMW, Inc. who filed these counterclaims in the action.

46. The Graham Order does not mention HomeSource or the White family at all.

47. RWS’s newsletter misleadingly and falsely implies that HomeSource and/or its owners were found “guilty” of negligent misrepresentations, but they are not even parties to this lawsuit, and the Graham Order deals with a motion for attorney’s fees.

48. RWS goes on to state in the newsletter: “Despite the ruling, **Furniture Distributors Inc sued Homesource again when Homesource failed to make any of the payments ordered** (Case 3:15-CV-00313).”

49. The text “Case 3:15-CV-00313” contains a hyperlink to a Complaint filed in the United States District Court for the Western District of North Carolina, *Furniture Distributors,*

Inc. v. James R. White, Jr.; James R. White, Sr.; Phyllis M. White; Gregory L. White; Courtney Murnane; Software-Support PMW, Inc.; The Homesource, Corp.; BBJ Corp., and Centerspec, LLC.

50. RWS falsely states that HomeSource was sued for a second time by Furniture Distributors, Inc., but HomeSource was not a party to the original Furniture Lawsuit.

51. RWS falsely states that HomeSource failed to make any of the payments ordered, but HomeSource was not ordered to make any payments and it was not a party to the prior lawsuit.

52. RWS misrepresented that HomeSource failed to make payments in order to intentionally disparage HomeSource's business and damages its relationship with its customers and potential customers.

53. RWS further misrepresented that Martin Salas was a consultant hired by HomeSource, but HomeSource never hired or entered into any contract with Martin Salas directly.

54. Upon information and belief, after HomeSource filed the initial complaint in this action, RWS continued to make false, misleading, and/or defamatory statements about HomeSource to HomeSource's customers, potential customers, and third parties.

C. RWS Misrepresented Security Vulnerabilities and Tried to Pose as a Customer to Acquire Access to HomeSource's Systems

55. On July 19, 2018, at 11:58 p.m., Jim Kane, CEO of RWS, emailed HomeSource and Ken Miele, of ADC, to point out a potential security hole and vulnerability in HomeSource's systems.

56. Less than two hours later, RWS emailed the July 20th Newsletter to HomeSource's customers which states: "Our investigation unearthed a possible major security concern with HomeSource sites." *See* Exhibit A.

57. The July 20th Newsletter contained a link to a short video where Jim Kane explains how he believes one could hack into HomeSource's system, and he provides the steps one could take in order to do it.

58. The video misrepresents the security of customers' files and alleges that they are publicly available, when in fact, HomeSource does not store customer information in this "bucket" or online folder.

59. Upon information and belief, an employee at RWS left a voicemail for HomeSource in which he posed as a potential customer named Tony Bosco, who claimed to be opening a store for furniture and appliances called Kensington Appliance and Furniture, in order to deceive HomeSource and gain access to their data and methods.

60. Upon information and belief, although "Tony Bosco" alleged that he was from the suburbs of Pittsburgh, his phone number traced back to an RWS number.

D. Cyber-Attack Doe Launched DoS and/or DDoS Attacks against HomeSource's Customers' Websites

61. In 2018, HomeSource moved hundreds of customers from RWS's platform to HomeSource's platform.

62. These customers are predominantly local retailers that sell appliances, electronics, and furniture through a brick and mortar store and a website.

63. HomeSource provides these customers with e-commerce solutions for their websites through its pricing-lookup tool and software.

64. Upon information and belief, RWS has delayed and/or ignored requests from RWS's former/current customers to have their domains released so they can be transferred to HomeSource's platform.

65. Beginning in August 2018, Cyber-Attack Doe deployed several DoS and DDoS attacks through the use of bots and/or programs that only targeted HomeSource's customers who also used to be customers of RWS.

66. In these DoS and DDoS attacks, the bots and/or programs would continually view the websites and run hundreds and thousands of searches in an effort to overload HomeSource's computer systems and software and crash the websites.

67. Upon information and belief, HomeSource has reason to believe that Cyber-Attack Doe's attacks were and are coming out of Scottsdale, Arizona, the same location as defendant RWS, due to the exponentially disproportionate volume of traffic coming out of the location.

68. Cyber-Attack Doe hid its operating system, browser, and many parts of its digital fingerprint when launching the attacks in order to conceal its identity.

69. Cyber-Attack Doe also deployed bots which are programmed to continually send hundreds and thousands of requests for service upon a single website in order to crash it, or at the very least, severely slow it down for other consumers trying to use the site.

70. Cyber-Attack Doe has launched thousands of DoS and/or DDoS attacks against HomeSource's customers since the beginning of August 2018.

71. The only HomeSource customers that have been victimized by these attacks were all former customers of RWS, as HomeSource's remaining customers were not targeted.

Count I – False and Misleading Advertising under the Lanham Act, 15 U.S.C. § 1125 (a)
against Defendant RWS

72. HomeSource repeats and incorporates all other paragraphs of this Complaint as if fully set forth herein.

73. Section 1125(a) of Title 15 of the United States Code states, in pertinent part, the following:

Any person who, on or in connection with any good or services, ... uses in commerce any word, term, name, symbol, ... or any false designation of origin, false or misleading description of fact, or false or misleading representation of fact... which – in commercial advertising or promotion, misrepresents the nature, characteristics, qualities... of another person's goods, services, or commercial activities, shall be liable in a civil action by any person who believes that he or she is or is likely to be damaged by such act.

74. RWS's use of "HomeSource" in connection with materially false and misleading statements about HomeSource's reputation, legal history, security, and the quality of its goods and services, constitutes commercial advertising that misrepresents the nature, characteristics, and qualities of HomeSource's goods, services, and commercial activities.

75. RWS's conduct in disseminating emails and newsletters and placing phone calls to HomeSource's customers and potential customers with materially false and misleading statements about HomeSource constitutes false advertising and unfair competition.

76. RWS's conduct constitutes false and misleading advertising in violation of 15 U.S.C. § 1125(a).

77. HomeSource has no adequate remedy at law. RWS's conduct has caused, and if not enjoined, will continue to cause irreparable damage to the rights of HomeSource, its brand, reputation and goodwill.

78. As a result of RWS's conduct, HomeSource has been damaged.

Count II – Defamation against Defendant RWS

79. HomeSource repeats and incorporates each paragraph of this Complaint as if set forth fully herein.

80. By engaging in the above-described conduct, RWS defamed HomeSource including, without limitation, by directly publishing and distributing emails and newsletters that deliberately, or at the very least negligently, (i) contain statements that are defamatory in nature and character; (ii) were published and disseminated by RWS to third parties, including HomeSource's customers and potential customers; (iii) were understood by their recipients to apply to HomeSource and to be defamatory; and (iv) caused special harm to HomeSource by virtue of such publications.

81. RWS's statements contained in the emails and newsletters impute both civil offenses and business and professional misconduct to HomeSource – including, but not limited to, allegations that HomeSource was found liable of negligent misrepresentation and allegations that HomeSource failed to pay a prior customer despite a court order.

82. RWS's statements contained in the emails and newsletters are the kind that would be particularly harmful to a business involved in e-commerce.

83. The statements contained in the emails and newsletters have caused and will continue to cause substantial pecuniary and reputational harm to HomeSource.

84. As a result, RWS is liable to HomeSource for damages caused by RWS's conduct.

Count III – Tortious Interference with Prospective Economic Advantage against Defendant RWS

85. HomeSource repeats and incorporates each paragraph of this Complaint as if set forth fully herein.

86. HomeSource had a protected interest in its reasonable expectation of economic advantage, as it relates to HomeSource's prospective economic interests with potential customers of its goods/services.

87. RWS willfully, maliciously, and intentionally interfered with HomeSource's prospective economic advantage by publishing materially false and misleading statements about HomeSource in newsletters and emails that RWS sent to HomeSource's potential customers, customers, and its customers' buyers.

88. RWS's conduct was without justification.

89. There is a reasonable likelihood that RWS's conduct caused HomeSource a loss of prospective economic gain.

90. As a direct and proximate result of RWS's conduct, HomeSource has been and continues to be damaged.

91. By reason of the foregoing, HomeSource is entitled to injunctive relief, treble damages, attorneys' fees and costs, and further relief as the Court deems just and proper.

Count IV – Tortious Interference with Contract against Defendant RWS

92. HomeSource repeats and incorporates each paragraph of this Complaint as if set forth fully herein.

93. RWS was fully aware of the contractual relationship existing between HomeSource's customers and HomeSource, including the fact that a valid and enforceable contract existed between these parties, and RWS was a not a party to this contractual relationship.

94. RWS willfully and intentionally interfered with the contractual relationship by publishing materially false and misleading statements about HomeSource in newsletters and emails that RWS sent to HomeSource's customers, and its customers' buyers.

95. RWS's conduct is without justification.

96. As a direct and proximate result of RWS's conduct, HomeSource has been and continues to be damaged.

97. By reason of the foregoing, HomeSource is entitled to injunctive relief, treble damages, attorneys' fees and costs, and further relief as the Court deems just and proper.

Count V – Common Law and Federal Unfair Competition against Defendant RWS

98. HomeSource repeats and incorporates each paragraph of this Complaint as if set forth fully herein.

99. RWS's conduct constitutes unfair competition, in that RWS is attempting to benefit commercially by stealing HomeSource's customers and publishing materially false and misleading statements about HomeSource.

100. RWS's wrongful conduct arises directly out of and is connected to its advertising activities.

101. Such acts constitute unfair competition against HomeSource under 15 U.S.C. § 1125.

102. HomeSource has been and continues to be damaged by RWS's activities and conduct. Accordingly, HomeSource is entitled to recover its damages, pursuant to 15 U.S.C. §1117(a).

103. Unless RWS's conduct is enjoined, HomeSource and its goodwill and reputation will suffer irreparable injury which cannot be adequately calculated or compensated solely by money damages.

104. By reason of the foregoing, HomeSource is entitled to injunctive relief, treble damages, attorneys' fees and costs, and further relief as the Court deems just and proper.

Count VI – Violation of Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(5)(A) against Defendant John Doe 1 (“Cyber-Attack Doe”) and John Doe 2 (“Hacking Doe”)

105. HomeSource repeats and incorporates each paragraph of this Complaint as if set forth fully herein.

106. Cyber-Attack Doe coordinated several DoS and DDoS attacks against HomeSource’s computers systems and HomeSource’s customers’ websites that were designed to interfere with interstate commerce by dramatically slowing down and/or crashing the websites.

107. Hacking Doe attempted to unlawfully and anonymously hack into HomeSource’s platform and obtain HomeSource’s customer data without authorization.

108. Through their conduct, Cyber-Attack Doe and Hacking Doe knowingly caused the transmission of a program, information, code, or command with the intent to cause damage, without authorization, to a protected computer system.

109. HomeSource’s computer system and customers’ websites are a protected computer under the CFAA because they are used in interstate commerce.

110. As a direct result of Cyber-Attack Doe’s and Hacking Doe’s conduct, HomeSource has suffered at least \$5,000 in damages in the past year through analyzing, investigating, and responding to the hacking, DoS, and DDoS attacks.

111. By reason of the foregoing, HomeSource is entitled to injunctive relief, damages, attorneys’ fees and costs, and further relief as the Court deems just and proper.

Count VII – Tortious Interference with Contract against Defendant John Doe 1 (“Cyber-Attack”), John Doe 2 (“Hacking Doe”) and John Doe 3 (“Fake Customer Doe”)

112. HomeSource repeats and incorporates each paragraph of this Complaint as if set forth fully herein.

113. Upon information and belief, the John Doe defendants were fully aware of the contractual relationship existing between HomeSource’s customers and HomeSource, including

the fact that a valid and enforceable contract existed between these parties, and the defendants were not a party to this contractual relationship.

114. Cyber-Attack Doe willfully and intentionally interfered with the contractual relationship by coordinating DoS and DDoS attacks against HomeSource's customers' websites that were designed to dramatically slow down and/or crash the websites, and designed to sever and/or interfere with the contractual relationship between HomeSource and its customers as a result.

115. Hacking Doe willfully and intentionally interfered with the customer relationship by attempting to unlawfully hack into HomeSource's system and obtain and compromise customer data without authorization.

116. Fake-Customer Doe willfully and intentionally interfered with the customer relationship by disparaging HomeSource's services to HomeSource's customers (without any basis for doing so) and falsely holding himself out as a real customer.

117. The John Doe defendants' conduct is without justification.

118. As a direct and proximate result of Does' conduct, HomeSource has been and continues to be damaged.

119. By reason of the foregoing, HomeSource is entitled to injunctive relief, treble damages, attorneys' fees and costs, and further relief as the Court deems just and proper.

120. HomeSource reserves its right to move to amend to assert additional claims for relief against John Does 1-3, based upon information as to their identity or identities, as discovery proceeds.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff HomeSource prays for relief and judgment, and requests that the Court:

(A) enter judgment against RWS and John Does 1-3 and in favor of HomeSource with respect to each claim for relief alleged in this Complaint;

(B) award HomeSource injunctive relief, treble damages and its costs and attorneys' fees, pursuant to the Lanham Act; and

(C) award such other and further relief as the Court deems just and proper.

Respectfully submitted,

FLASTER/GREENBERG P.C.

Dated: September 4, 2018

By: /s/ Alexis Arena

Alexis Arena, Esq.

Eric R. Clendening, Esq.

1810 Chapel Avenue West

Cherry Hill, NJ 08002

(856) 661-1900

Fax: (856) 661-1919

alexis.arena@flastergreenberg.com

Attorneys for Plaintiff